Safeguard Privilege Manager for Windows 4.7

Quick Start Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Safeguard Privilege Manager for Windows Quick Start Guide
Updated - 25 September 2024, 19:07

For the most recent documents and product information, see Online product documentation.

Contents

1

About this guide

Welcome to the Safeguard Privilege Manager for Windows Quick Start Guide. Safeguard Privilege Manager for Windows lets system administrators grant selected privileges to users so they can update their own PCs, reducing help desk calls while maintaining a secure network. This guide instructs system administrators on how to set up the Safeguard Privilege Manager for Windows Console, Server, and Client. This guide also provides an overview of the key features and wizards of the product.

For more information, refer to these additional resources:

For system administrators

- *Safeguard Privilege Manager for Windows Administration Guide*: Learn how to use Safeguard Privilege Manager for Windows. Find in-depth instructions on how to prepare your environment for least privileged use, maintain a least privileged environment, run reports, and interface with Microsoft tools.
- Safeguard Privilege Manager for Windows Console: Find more information on the **Getting Started** screen under the **Additional Resources** tab.

For end users with the Privilege Manager Client service installed on their computers

- *Safeguard Privilege Manager for Windows User Guide*: Learn the basics of using Safeguard Privilege Manager for Windows for Windows, including how to use Self-Service Elevation, Instant Elevation, and view rules.

System requirements

Before you begin using Safeguard Privilege Manager for Windows, make sure that you meet the minimum hardware, software, network and permission requirements of the product. For more information, see *System Requirements* in the *Safeguard Privilege Manager for Windows Release Notes*.

3

Components

There are three software components included with Safeguard Privilege Manager for Windows:

- the Console
- the Server
- the Client

Console

The Safeguard Privilege Manager for Windows Console, installed via `PAConsole_Pro.msi`, is a management application. It is installed on a domain computer (server or workstation) and is used to create and manage rules within the Group Policy. Any user who has permission to edit a GPO can use the Console to set privileges.

Server

The Safeguard Privilege Manager for Windows Server, installed through the Console, is a service which has several functions. It can deploy the Client, collect and report on data, and discover and process applications that require elevated privileges.

Client

The Safeguard Privilege Manager for Windows Client, installed through `PAClient.msi`, is a service that runs on each client computer. It applies the rules created in the Console by monitoring processes as they are launched on the Client and elevates or lowers the privileges for processes that are configured to be monitored. This is done by injecting an administrative token into the process or revoking it.

Microsoft Active Directory and Group Policy are used to distribute Safeguard Privilege Manager for Windows rules to client computers.

Privilege Manager can modify privileges only for a standard user account, not a guest account. Elevated privileges can be revoked even if the user is a local admin.

Preparing your environment for least privileged use

Prepare your environment for least privileged use by installing Safeguard Privilege Manager for Windows, configuring reporting, discovery, and remediation settings, configuring approved privileged applications, and removing local admin rights.

Product Licensing

For information on editions and applying a license, refer to the *Safeguard Privilege Manager for Windows Administration Guide*.

Safeguard Privilege Manager for Windows licenses are compatible with only a single major version of the product (for example, 3.x or 4.x). This means that existing 3.x licenses are not valid after upgrading to a 4.x build.

Therefore, when upgrading to a new major version, existing customers must obtain a new license file using the License Assistance portal to properly register the product after upgrade.

NOTE: Safeguard Privilege Manager for Windows does not transmit license data automatically to One Identity. Instead, you must update the product license manually. For more information, see *Product licensing* in the *Safeguard Privilege Manager for Windows Release Notes*.

Configuring access to ports, websites, and processes

Your firewall must allow the Safeguard Privilege Manager for Windows Console to access the following domains on ports **80** (non-SSL) and **443** (SSL). In addition to those ports, the Safeguard Privilege Manager for Windows uses a configurable port for the data collection service (**8003** by default), to receive information from managed target devices.

Domain	Used for
download.microsoft.com	Microsoft updates
webservices.scriptlogic.com	Safeguard Privilege Manager for Windows web server
support.oneidentity.com	One Identity Support Portal
dams-service.kace.com	Data collection

The following features and processes must be allowed through the firewall on target devices:

- Discovering users with local administrative rights:
  - Windows Management Instrumentation (WMI)
  - Distributed Component Object Model (DCOM)
  - File and Printer Sharing
  - Remote Administration
- Testing rules:
  - Windows Management Instrumentation (WMI): dllhost.exe
  - Host process for Windows services: svchost.exe for 32-bit OS and %SystemRoot%\SysWOW64\svchost.exe for 64-bit OS

Installing the Console

For instructions on using the Console Windows Installer file, see *Using the Console Windows Installer file* in the *Safeguard Privilege Manager for Windows Administration Guide*.

Configuring the Server

For instructions on using the Server Configuration Wizard, see *Using the Server Configuration Wizard* in the *Safeguard Privilege Manager for Windows Administration Guide*.

Offline installation of the Server and Data Collection service

Safeguard Privilege Manager for Windows does not directly support offline installation. However, you can set up the Server and Data Collection service of the Console if you install some dependencies manually beforehand.

To set up the Server and Data Collection service offline

1. Install the following components:
    - Microsoft System CLR Types for Microsoft SQL Server 2014
        - 32-bit
        - 64-bit
    - Microsoft SQL Server 2014 Shared Management Objects
        - 32-bit
        - 64-bit
    - Microsoft SQL Server 2014 SP2 Express
        - 32-bit
        - 64-bit
2. Set up the SQL Server manually. For example, you can run the following command to initiate the SQL Server installer with some pre-configuration in place:

    ```
    SQLEXPR_2014_ENU.exe /IACCEPTSQLSERVERLICENSETERMS /ACTION=Install
    /FEATURES=SQL /INSTANCENAME=PAReporting /SECURITYMODE=SQL /SAPWD=<sql-system-
    admin-password> /SQLSVCACCOUNT=<sql-service-account>
    /SQLSYSADMINACCOUNTS="BUILTIN\ADMINISTRATORS" /AGTSVCACCOUNT=<sql-service-
    account> /TCPENABLED=1 /SQLSVCPASSWORD=<sql-service-password>
    /AGTSVCPASSWORD=<sql-service-password>
    ```
3. Once you are done, you can configure the server in the Console using the **Use an existing SQL Server instance** option during server setup.

Installing the Client

For instructions on using the Client Deployment Settings Wizard, see *Using the Client Data Collection Settings Wizard* in the *Safeguard Privilege Manager for Windows Administration Guide*.

Configuring reporting, discovery, and remediation settings

Access the wizards described below under the **Setup Tasks** tab on the **Getting Started** screen.

Configuring Client data collection

Run the Client Data Collection Settings Wizard to compile reports, support discovery, and launch on-demand features. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab, and double-click the **Client Data Collection Settings Wizard**. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

Configuring Instant Elevation

To grant on-demand administrative privileges to a group of trusted users and audit their actions, use the Instant Elevation Wizard. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Instant Elevation Wizard**. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

Configuring Self-Service Elevation

To enable users to request permissions to use privileged applications, use the Self-Service Elevation Request Settings Wizard. Whenever a user attempts to run an application which requires administrative permissions for which they do not have rights, they are asked if they would like to send a request to their administrator for permission to run it. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Self-Service Elevation Request Settings Wizard**. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

NOTE: In some cases, Self-Service Elevation and Blacklist rules can be configured for the same target application. In this case, Blacklisting takes precedence over Instant Elevation and prevents the application from starting. For more information about creating Blacklisting rules, see *Using the Create Rule Wizard* in the *Safeguard Privilege Manager for Windows Administration Guide*.

To filter out Application Discovery data

1. Click **Next** to use the **Filters** tab to filter out Application Discovery data according to different application specific criteria.
2. On the **Filters** tab, select the check box to enable application filters.
3. Enter filter criteria in one or more of the available boxes (**Executable path contains**, **Product name contains**, **Publisher name contains**, and **File description contains**).

   NOTE: An application only needs to meet a single filter criteria to filter out its Application Discovery data. To enter multiple criteria in each filter field, use commas (,) as delimiters.

NOTE: The Safeguard Privilege Manager for Windows Client does not transmit any Application Discovery data for one or more applications that meet any of the existing filter criteria.

Configuring privileged application discovery

Use the Privileged Application Discovery Settings Wizard to collect information about the privileged applications used over your network during a specified time period. By default, once this feature is enabled, it is set to collect information for two weeks, but you can adjust the setting. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Privileged Application Discovery Settings Wizard**. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

Configuring approved privileged applications

Processing discovered privileged applications

Use the **Privileged Application Discovery** screen under the **Discovery & Remediation** tab to process the privileged applications that were reported by the client computers. If these applications are approved and need to continue even after the least-privileged environment is in place, use this screen to automatically create and assign Elevation rules to appropriate groups. If a discovered application is not approved for use in the least privileged environment, you can ignore these applications and they will no longer display. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

6

Deploying rules

To create the default rules provided by Privilege Manager, use the **Create GPO with Default Rules Wizard**. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click **Create GPO with default rules**. Follow the prompts or see the *Safeguard Privilege Manager for Windows Administration Guide* for more information.

Removing local admin rights

The last step in preparing your environment for least privileged use is to remove administrative access from users who no longer require it.

Using the Active Directory Users and Computers utility

To scrub the Domain Administrators group of users that should no longer have administrative rights to every computer in the domain, use the native Active Directory Users and Computers utility of the supported Windows Server operating systems.

To remove users from the Domain Administrators group,

1. Select **Domain Admins Properties** > **Members tab** > **Remove**.
2. Click **Discover Accounts in local Administrator groups** to discover users and domain groups with local administrator rights.

   NOTE: By default, the search results will only include domain users and domain groups. However, you can optionally opt to include local and built-in (for informational purposes only) users.

8

Using the Users with Local Admin Rights screen

To discover which domain users have been assigned to the local Administrators group on client computers, and then remove them, under the **Discovery & Remediation** tab of the Console, select the **Users with Local Admin Rights** screen. For more information, see *Safeguard Privilege Manager for Windows Administration Guide*.

Maintaining a least privileged use environment

Maintain a least privileged use environment by processing Self-Service Elevation requests, using the **Console Email Configuration** screen, and using group policy settings.

Processing Self-Service Elevation Requests

Monitor and process Self-Service requests from users using Self-Service Notifications and the **Self-Service Elevation Requests** screen under the **Discovery & Remediation** tab. You can approve or deny requests for access to run privileged applications. If approved, an Elevation rule is automatically generated for each request. For step-by-step instructions, see the *Safeguard Privilege Manager for Windows Administration Guide*.

Using the Console Email Configuration screen

If you want Safeguard Privilege Manager for Windows to send an email message to the user after approving or denying their Self-Service Elevation request, configure the settings using the **Setup Tasks** > **Console Email Configuration** screen. For more information, see the *Safeguard Privilege Manager for Windows Administration Guide*.

10

Using Group Policy Settings

To create custom Elevation rules or modify existing ones for your environment, use the Group Policy Settings screens. To modify the settings for advanced features at the GPO level, use the **Advanced Policy Settings** tab. For more information, see the *Safeguard Privilege Manager for Windows Administration Guide*.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product